ORIGINAL

Paul R. Kiesel, Esq. (SBN 119854)
KIESEL BOUCHER LARSON LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211
kiesel@kbla.com
Telephone: (310) 854-4444
Facsimile: (310) 854-0812

HORWITZ, HORWITZ & PARADIS
Attorneys at Law
570 Seventh Avenue, 20th Floor
New York, NY 10018
Telephone: (212) 986-4500
Facsimile: (212) 986-4501
(additional counsel listed on signature page)

E-Filing

FILED
DEC 13 2011
RICHARD W. WIEKING
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ADR

$
#4
Fee
Sl

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

PSG

YONATAN WADLER, individually and on behalf of all others similarly situated,

Plaintiff,

v.

CARRIER IQ, INC.
A Delaware Corporation.

Defendant.

CASE NO: CV 11-06278

CLASS ACTION COMPLAINT FOR:

(1) VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT;

(2) VIOLATIONS OF THE CALIFORNIA PRIVACY ACT;

(3) TRESPASS TO CHATTEL;

(4) VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW; and

(5) VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT

FAXED

Plaintiff Yonatan Wadler ("Plaintiff") individually and on behalf of all others similarly situated, by his undersigned counsel, alleges the following upon personal knowledge as to his own acts and upon information and belief as to all other matters. Plaintiff's information and belief are based upon the investigation conducted by counsel.

NATURE OF THE ACTION

1. Plaintiff brings this action individually and as a class action against Carrier iQ, Inc. ("CiQ") on behalf of himself and all others who either (i) own an electronic device, including but not limited to, smartphones, traditional feature phones, tablets, and electronic-readers (collectively the "Electronic Devices") in which CiQ Mobile Intelligence software ("CiQ's software") was installed, or (ii) own an Electronic Device that sent an electronic communication to an electronic device in which CiQ's software was installed or received an electronic communication sent from an electronic device in which CiQ's software was installed.

2. Through its software, CiQ has been illegally intercepting, collecting, and sharing the electronic communications that are sent and received by the Electronic Devices in which CiQ is installed for several years.

3. Such electronic communications include every key that a user presses, every text message and email sent and received by the user, and all Internet browser usage and history while using the Electronic Devices.

4. This deeply intrusive surveillance campaign has occurred unbeknownst to Plaintiff and Class members, who were not given an opportunity to provide informed consent to such surveillance. The nature and extent of CiQ's intrusive and comprehensive surveillance was not disclosed to Plaintiff and the members of the Class.

5. As a result of the facts alleged herein, Defendant has violated federal and state laws governing the protection of Plaintiff's and Class members' privacy.

\\\

\\\

PARTIES

6. Plaintiff Yonaton Wadler is a citizen of the State of New York. He purchased an HTC 4G smartphone with cellular service provided by Sprint Nextel Corporation ("Sprint") and, unbeknownst to Plaintiff, his device had CiQ's electronic interception software installed in it.

7. Defendant Carrier iQ Inc. maintains its principal executive offices at 1200 Villa Street, Suite 200, Mountain View, CA 94041. CiQ, established in 2005, develops software that CiQ, cellular service providers ("carriers"), and original equipment manufacturers ("OEMs") use to collect and intercept data and communications sent or received by a wide variety of Electronic Devices.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over the claims asserted in this action pursuant to 28 U.S.C. § 1331 because Plaintiff's claims arise under the laws of the United States, including the Federal Wiretap Act, 18 U.S.C. §§ 2510 *et seq.*

9. This Court also has subject matter jurisdiction over the claims asserted in this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332. Plaintiff, a citizen of New York, brings claims on behalf of a nationwide class against Defendant, a citizen of California and the aggregate claims of Plaintiff and members of the Class exceed the sum or value of $5,000,000.

10. This Court has personal jurisdiction over Defendant because Defendant maintains sufficient contacts in this jurisdiction.

11. Venue is proper in this District because Defendant maintains its principal executive offices and headquarters in this District, and a substantial part of the events giving rise to the claim occurred in this District.

\\\

\\\

\\\

\\\

SUBSTANTIVE ALLEGATIONS

Background on the Smartphones and other Electronic Devices

12. On its website, CiQ estimates that it has installed its CiQ software in more than 140 million Electronic Devices.

13. A "smartphone" is a mobile phone that offers wireless internet connectivity and more advanced computing ability than a traditional cellular phone. Because smartphones have many of the features possessed by computers, smartphones require an operating system ("OS") to function. An operating system is software that consists of programs and data that manages computer hardware resources and provides common services for efficient execution of various application software.

14. A tablet computer is a class of small mobile computers, usually having a touchscreen or pen-enabled interface. An e-reader is an electronic device for reading content, such as books, newspapers and documents in digital format. Both e-readers and tablets have wireless connectivity for downloading content and conducting other Web-based tasks.

15. The capabilities of the smartphones and the other Electronic Devices make information accessible at the user's fingertips. CiQ has capitalized on this technology by using it to surveil Electronic Device users illegally 24 hours per day 7 days per week, as admitted by CiQ's own Vice President of Marketing, Andrew Coward.

16. According to CiQ's website, "Our software is embedded by device manufacturers along with other diagnostic tools and software prior to shipment."

CiQ's Illegal Surveillance and Communication Interception

17. CiQ's software enables CiQ to read, intercept, and record all communications that are sent and received by an electronic device in which CiQ's software is installed. Rather euphemistically, CiQ refers to its software and data interception services as "Mobile Intelligence."

///

18. Andrew Coward described the surveillance, data interception, and data collection provided through CiQ's software in detail when he stated in relevant part:

> The answers lie within the handset itself because the handset holds untapped information about what actually happens. Getting out and exploiting this information is what we call 'mobile intelligence.' To extract it, we work with handset manufacturers to embed an agent inside the phone—an agent that works pretty much like a rewind button and records when things go wrong and brings together the data to make them right again. So far this agent has shipped on 150 million devices. And not just on handsets, but on tablets, readers, and data sticks to provide detailed 'mobile intelligence' on how well and where networks, devices, and applications are really performing. . . .

19. CiQ's website states in relevant part:

> Carrier IQ delivers Mobile Intelligence on the performance of mobile devices and networks to assist operators and device manufacturers . . . . We do this by counting and measuring operational information in mobile devices – feature phones, smartphones and tablets. . . .

20. A CiQ press release described the illegal interception in great detail:

> IQ Insight Experience Manager gives wireless carriers and mobile device manufacturers an unprecedented, objective view into what is actually happening on mobile subscribers' devices – including quality of service, application usage and the related experience – as it occurs, at the point of delivery and use.
>
> * * *
>
> Experience Manager takes customer experience profiling to an advanced level with multiple levels of granularity, from the entire population, to comparative groups, down to individual users
>
> * * *
>
> **IQ Insight Experience Manager uses data directly from the mobile device to give a precise view of how the services and the applications are being used, even if the phone is not communicating with the network.**
>
> * * *

> **The solution can be applied by Carrier IQ's existing customers to their own deployed base of handsets which already have the company's core technology embedded in the device**, and it can also be applied to new devices as they are introduced. In total, Carrier IQ's core technology is already embedded on more than 35 million handsets globally. (Emphasis added).

CiQ's Illegal Interception Scheme is Publicly Exposed

21. In reality, CiQ's "Mobile Intelligence" amounts to illegal surveillance and interception conducted without the consent of the Class members.

22. Electronic Device users were unaware that CiQ was illegally intercepting their communications until a systems administrator, Trevor Eckhart, publicly revealed the truth.

23. Trevor Eckhart explained that CiQ's software is a rootkit. A rootkit is software that enables continued privileged access to a computer while actively hiding its presence from administrators by subverting standard operating system functionality or other applications.

24. He discovered that CiQ's software enables CiQ continued, privileged access to the smartphones. CiQ's software is hidden in nearly every part of the smartphones, including the kernel. The kernel is the main component of most computer operating systems; it is a bridge between applications and the actual data processing done at the hardware level. CiQ's software also subverts standard operating system functionality.

25. Specifically, Trevor Eckhart discovered that the CiQ's software was running in his HTC Evo 3D smartphone. However, his smartphone would not allow him to disable or remove CiQ's software.

26. Trevor Eckhart connected his smartphone to a device that allowed him to observe the activity of the CiQ software, which is referred to as USB debugging to read logcat logs created by the CiQ program. The debugging log files were not only stored in the operating system of the phone, but they were also transmitted to CiQ.

A. CiQ Records Every Keystroke and Action

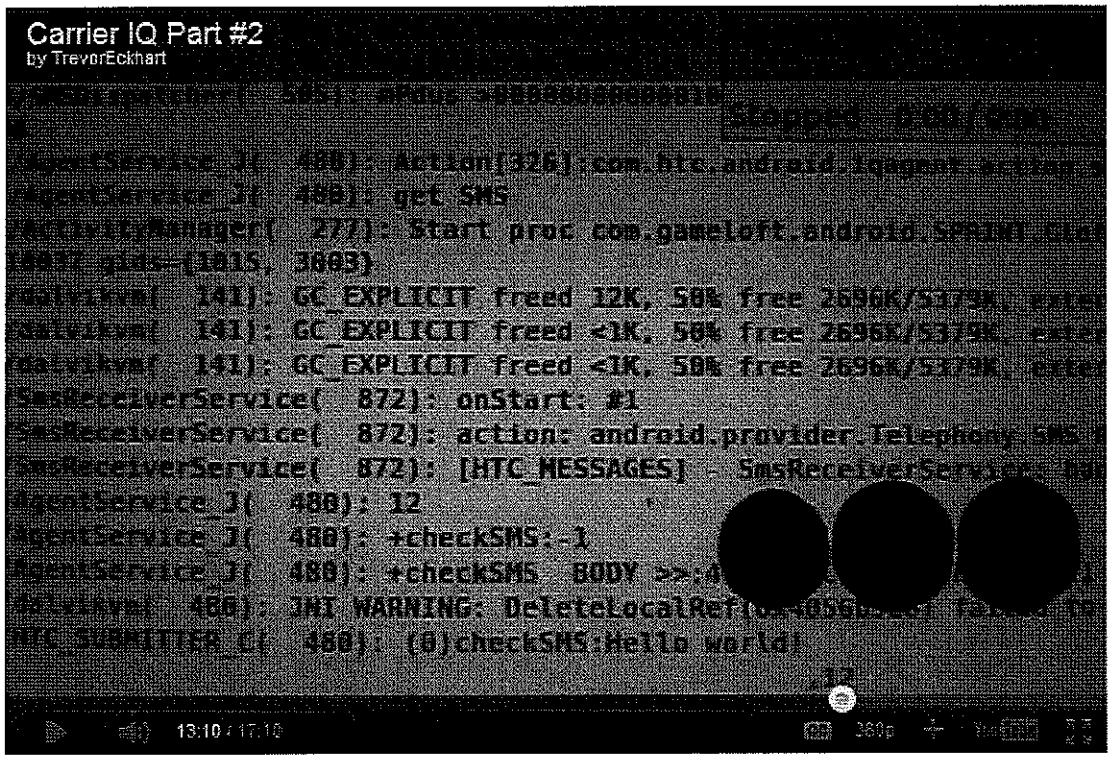
27. By depressing every button on his smartphone, Mr. Eckhart demonstrated that a specific code called a "wkeycode" for each button was recorded and was sent to CiQ. This enabled CiQ to recognize, read, and record every letter and word he typed into his smartphone.

28. In addition, every action he took with his phone, such as turning it on or off, had an action identifier. The action identifiers were also sent to CiQ contemporaneously with their occurrence.

B. CiQ Intercepts Every Text Message Sent and Received

29. Using the USB debugger, Trevor Eckhart was able also to observe that every time he sent or received a text message, CiQ was able to recognize that a text message was sent or received and illegally intercept the text message. CiQ's software would then read and display the actual text of the text message to CiQ, as depicted in **Figure 1** below at the bottom of the picture. In Trevor's testing, that message was "Hello World!"

Figure 1



30. CiQ's interception software is so sophisticated that it actually reads all text messages sent from, or received by, an Electronic Device **before** the users of those Electronic Devices are able to read them.

31. All of this information is then transmitted to not only CiQ, but also all of CiQ's customers, which include OEMs and carriers.

32. CiQ's interception software is not unique to HTC smartphones. Rather, CiQ software performs equivalent interception in any Electronic Device in which it is installed. CiQ, by its own admission, is a data collector and data aggregator for its customers.

C. CiQ Illegally Intercepts Internet Communications on Private Wi-Fi Networks

33. Trevor Eckhart also discovered that CiQ also illegally intercepted all Internet browsing history while he was using his own wireless network, not his carrier's network.

34. When Mr. Eckhart entered search terms into Google.com and performed an Internet search, CiQ's software once again illegally intercepted these electronic communications and actually read and displayed the search as depicted by **Figure 2.**

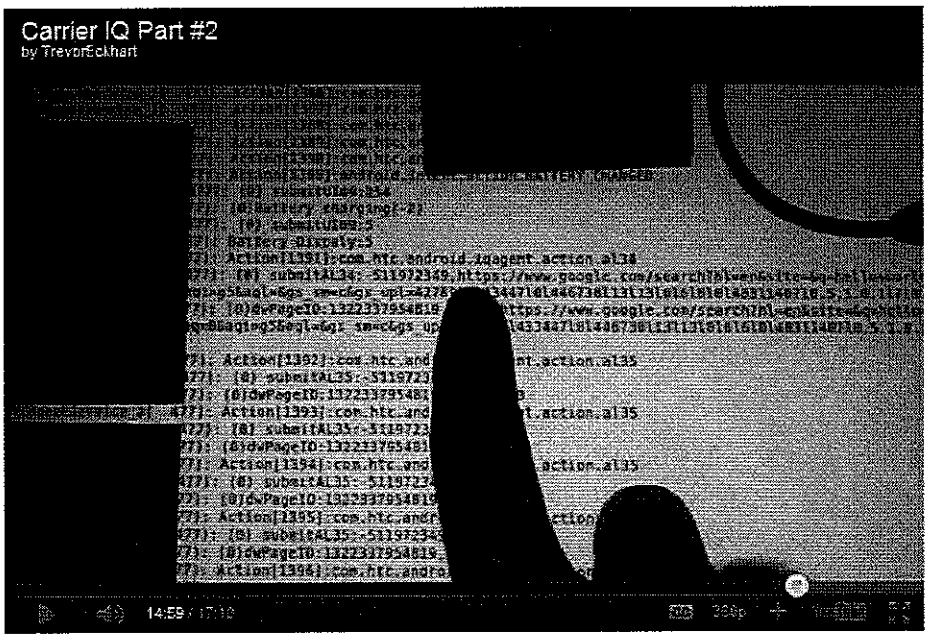


Figure 2

35. When a user enters search terms into a search engine or enters a URL into the navigation toolbar, CiQ's software reads, records and transmits this information to CiQ. CiQ, by its own admission, collects this data for its customers as well.

36. Eckhart discovered that, despite his efforts to disable CiQ software, it was incapable of being disabled.

D. CiQ's Software Could Not be Removed

37. Eckhart discovered that, despite his efforts to disable CiQ software, it was incapable of being disabled. Eckard had to design a new application specifically to remove the CiQ's software because no other application with such power existed.

38. CiQ's software is programmed into the read only memory ("ROM") of the smartphones' operating systems. Removing CiQ from the ROM requires gaining "root" access to the ROM, which amounts to "unlocking" the ROM and is a risky procedure that can damage the device.

39. As reported in the Wall Street Journal on December 5, 2011, by Tom Loftus,

> Because Carrier IQ software is deeply integrated with handset firmware, users would be required to attain special device privileges in order to remove it. Side effects of this process have the potential to put users at further risk of malware infection while making devices ineligible to receive firmware updates in the future.

40. The only other option to remove CiQ's software from the smartphone is to remove and replace the ROM that is installed in the device by the manufacturer. The user would have to obtain a newly designed ROM from another source.

41. CiQ's software also creates log catalogue files that that are stored within the allocation of the operating system. These log catalogue entries consume space that could be used for other applications and noticeably reduces the speed at which the smartphone operates. After the log catalogue files are removed from the device, an improvement in the rate of operation speed of the device is easily apparent.

E. CiQ's Half-Hearted Effort to Suppress Trevor Eckhart's Discoveries

42. When CiQ became aware that Mr. Eckhart was about to alert the public about CiQ's illegal scheme, CiQ attempted to squelch Mr. Eckhart's activities by serving him with a Cease-and-Desist letter, giving him two days to respond, and threatening to seek damages from him if he did not cease his activities.

43. Undeterred by CiQ's threats, however, Eckhart hired the Electronic Frontier Foundation, an organization committed to protecting privacy, to defend him. Soon thereafter, CiQ withdrew its Cease-and-Desist letter and apologized to him by stating that CiQ was "deeply sorry for any concern or trouble" that CiQ's Cease-and-desist letter may have caused Eckhart.

44. Desiring to inform the public, Trevor posted his testing on YouTube.com. His YouTube.com video of the software in action stunned many as it showed CiQ's software logging information, including text messages, as the information is tapped onto the phone keyboard.

45. After the shocking revelation, three major carriers admitted that CiQ's software is embedded in their smartphones. AT&T publically acknowledged use of CiQ's software. T-Mobile has also confirmed that CiQ's software is embedded in its devices. T-Mobile, contacted by msnbc.com, said late Thursday, December 2, 2011, it uses Carrier IQ. In addition, Sprint Spokeswoman, Stephanie Vinge, admitted on behalf of Sprint that CiQ's software is embedded in its smartphones and that CiQ supplies data to Sprint.

46. The controversy caused by Trevar Eckhart's revelations also prompted Senator Al Franken to send a letter to AT&T, HTC, Samsung, and Sprint Nextel, after they acknowledged their use of CiQ's software, asking them to explain what they do with the information that CiQ intercepts.

Any Purported "Opt Out" or "Consent" is Deceptive and Invalid

47. Carriers themselves do not disclose in their contracts the kind of surveillance that Trevor Eckhart has shown CiQ to be performing.

48. Furthermore, CiQ has never entered into any agreement with Electronic Device users, let alone obtained their consent to intercept their electronic communications.

49. Moreover, no provision in any contract or service agreement of any electronic device in which CiQ is installed discloses to the user that CiQ engages in the following: (i) CiQ will read and intercept all text typed into the electronic device; (ii) CiQ will read and intercept all of the content of the user's text messages and emails, sent or received; and (iii) CiQ will read and intercept all internet browsing history.

50. Without any disclosure of the intrusive and comprehensive nature of CiQ's communication interception, data collection, and surveillance, Plaintiff and Class members were not capable of providing informed consent to CiQ.

User Outrage Over the Illegal Interception of Their Communications

51. Plaintiff and Class members reasonably expected that text messages, emails, and Internet browsing habits were private and confidential. They did not expect or have knowledge that CiQ would illegally intercept and read their private communications, much less share them with CiQ's customers.

52. As one incensed smartphone user exclaimed, "Stay out of my phone! And reading my messages, everything I type even my id/passwords helps you support me how? You say my information is secured, how and why would I trust you? You don't give any option to opt-out or remove your spyware, and don't inform anyone what you doing upfront, [expletive deleted]. I hope you get sued you [expletive deleted]."

53. Another smartphone user complained "A video by the aptly named Andrew COWARD, pushing this program that has been lurking in my phone recording every keystroke, website and message I get. Just how does this benefit me? I don't remember signing up for this, and I certainly never gave you any sort of permission to receive MY personal information that I pay a hefty amount per month to be able to send and receive on MY phone. How you skirt legalities I haven't a clue, but I hope a lawsuit

is put together soon to put you out of business."

54. Yet another user echoed these sentiments, "OUT...OUT...STAY OUT OF MY PHONE,LIERS...LIERS...LIERS...[sic]-DONT YOU DARE TO SAY WE DONT UNDERSTAND [*]>>OFF...OUT THIEVES."

55. The following particular complaint reflects the concerns shared by other Class members: "The reasons everyone are so up in arms about this: 1) The data you collect goes well beyond data you need to help carriers support hardware/software. Why do they need my text messages, google searches, and unencrypted login/password details for my banking???? 2) You went to great lengths to hide this software on phones and prevent users from turning it off. 3) Now that it has been exposed, you are backpedaling and doing damage control after threatening to sue a user for simply exposing you." [1]

56. Outraged victims have posted thousands of other similar complaints on the Internet.

CLASS ACTION ALLEGATIONS

57. Plaintiff brings this action both individually and as a class action pursuant to Fed. R. Civ. P. 23(a) and 23(b)(3) against Defendant, on his own behalf and on the behalf of all others who either (i) own an Electronic Device in which CiQ's software was installed, or (ii) own an Electronic Device that sent an electronic communication to an electronic device in which CiQ's software was installed or received an electronic communication sent from an electronic device in which CiQ's software was installed.

58. Members of the Class are so numerous that joinder of all members would be impracticable. Plaintiff estimates that there are more than 140 million members of the Class.

\\\

[1] User complaints are unedited to maintain their authenticity.

59. There are questions of law and fact common to all the members of the Class that predominate over any questions affecting only individual members, including:

a. Whether Defendant intercepted Plaintiff's and Class members' electronic communications;

b. Whether Defendant's interceptions of Plaintiff's and Class members' electronic communications were intentional;

c. Whether Defendant's interceptions of Plaintiff's and Class members' electronic communications were without consent;

d. Whether Defendant obtained and continues to retain valuable information from Class members;

e. Whether, because of Defendant's misconduct, Plaintiff and other Class members are entitled to damages, restitution, equitable relief, injunctive relief, or other relief, and the amount and nature of such relief.

60. The claims of Plaintiff are typical of the claims of the members of the Class. Plaintiff has no interests antagonistic to those of the Class, and CiQ has no defenses unique to the Plaintiff.

61. Plaintiff will protect the interests of the Class fairly and adequately, and Plaintiff has retained attorneys experienced in complex class action litigation.

62. A class action is superior to all other available methods for this controversy because:

a. the prosecution of separate actions by the members of the Class would create a risk of adjudications with respect to individual members of the Class that would, as a practical matter, be dispositive of the interests of the other members not parties to the adjudications, or substantially impair or impede their ability to protect their interests;

b. the prosecution of separate actions by the members of the Class would create a risk of inconsistent or varying adjudications with respect to the

individual members of the Class, which would establish incompatible standards of conduct for Defendant;

c. Defendant acted or refused to act on grounds generally applicable to the Class; and

d. questions of law and fact common to members of the Class predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of the controversy.

63. Plaintiff does not anticipate any difficulty in the management of this litigation.

COUNT I

Violation of the Electronic Communications Privacy Act
Title 18 United States Code, Section 2510, *et seq.* (Wiretap Act)

64. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

65. Defendant intercepted, tracked and recorded Plaintiff and Class Members' electronic communications on Plaintiff and Class Members' Electronic Devices by and through the use of Defendant's Carrier IQ software application. Defendant used this software application to acquire the contents of Plaintiff and Class Members' communications, thereby diverting and transferring information containing and constituting the substance, purport, and meaning of Plaintiff and Class Members' communications.

66. Defendant's conduct was in violation of Title 18, United States Code, Section 2511(1)(a) because Defendant intentionally intercepted and endeavored to intercept Plaintiff and Class Members' electronic communications.

67. Defendant's conduct was in violation of Title 18, United States Code, Section 2511(1)(d) in that Defendant used and endeavored to use the contents of Plaintiff and Class Members' electronic communications, knowing and having reason to

know that the information was obtain through interception in violation of Title 18, United States Code Section 2511(1).

68. Defendant's conduct was knowing and intentional in that Defendant designed and operated its Carrier IQ software application described herein and executed this software application specifically for the purpose of engaging in the interceptions that Defendant did, in fact, carry out.

69. Defendant was not a party to the respective communications between Plaintiff and Class Members and websites, which Defendant monitored in-process.

70. Defendant's interception processes were invisible and unknown to Plaintiff and Class Members.

71. Defendant failed to disclose its interception processes to Plaintiff and Class Members.

72. Because Defendant's interception processes were invisible and undisclosed, any consent Defendant received to participate in Plaintiff and Class Members' communications did not constitute consent to Defendant's interception.

73. Only Plaintiff and Class Members possessed the authority to consent to another party's interception of their electronic communications.

74. Defendant's interception was therefore undertaken without the consent of any party to the communications that Defendant intercepted.

75. Defendant's tracking and interception of Plaintiff and Class Members' electronic communications were not necessarily incident to Defendant's rendition of services or protection of rights or property.

76. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members' electronic communications were intercepted and intentionally used in violation of Title 18, United States Code, Chapter 119.

77. Accordingly, Plaintiff and Class Members are entitled to such preliminary and other equitable or declaratory relief as may be just and proper.

///

78. Plaintiff and Class Members are also entitled to damages computed as the greater of: (i) the sum of actual damages suffered by Plaintiff and Class Members plus Defendant's profits made through the violative conduct herein; (ii) statutory damages for each Class Member of $100 a day for each day of violation; or (iii) statutory damages of $10,000 per individual.

79. Plaintiff and Class Members are also entitled to and request Defendant's payment of punitive damages.

80. Plaintiff and Class Members are also entitled to and hereby request Defendant's payment of reasonable attorneys' fees and other litigation costs reasonably incurred.

COUNT II
Violation of the Privacy Act
California General Laws, Chapter 214, Section 1B

81. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

82. Defendant illegally intercepted, tracked and recorded Plaintiff and Class Members' electronic communications as described herein.

83. Through the use of Defendant's Carrier IQ software application described herein, Defendant disclosed to third parties, and/or caused to be disclosed to the other third parties, Plaintiff and Class Members' Web-browsing, texting and calling information, which included facts of a highly private, sensitive, personal or intimate nature.

84. Defendant did so repeatedly throughout the Class Period.

85. Defendant did so knowing and intending to engage in conduct that Plaintiff and Class Members did not reasonably expect.

86. Defendant did so knowing Plaintiff and Class Members reasonably believed their privacy was protected. Defendant did so intending to circumvent the measures Plaintiff and Class Members' had taken to protect their privacy.

///

87. Defendant did so knowing its actions would seriously diminish, intrude upon, and invade Plaintiff and Class Members' privacy.

88. Defendant did so intending to seriously diminish, intrude upon, and invade Plaintiff and Class Members' privacy.

89. Defendant did so in a manner designed to evade detection by Plaintiff and Class Members.

90. Defendant had no legitimate, countervailing business interest in engaging in such conduct.

91. Defendant' actions did unreasonably, substantially, and seriously interfere with Plaintiff and Class Members' privacy.

92. In addition, Defendant's conduct has caused, and continues to cause, Plaintiff and Class Members irreparable injury. Unless restrained and enjoined, Defendant will continue to commit such acts. Plaintiff and Class Members' remedy at law is not adequate to compensate them for these inflicted, imminent, threatened, and continuing injuries, entitling Plaintiff and Class Members to remedies including injunctive relief.

93. Plaintiff and Class Members are entitled to equitable relief that includes Defendant's cessation of the illegal conduct alleged herein.

94. Plaintiff and Class Members are entitled to equitable relief that includes an accounting of what personal information of theirs was collected, used, merged, and further disclosed to whom, under what circumstances, and for what purposes.

95. As a proximate and direct result of Defendant's invasion of privacy, Plaintiff and Class Members were harmed.

96. Plaintiff and Class Members are therefore entitled to damages in an amount to be determined at trial.

97. Plaintiff and Class Members request such other preliminary and equitable relief as the Court deems appropriate.

///

COUNT III

Trespass to Chattel

98. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

99. The common law prohibits the intentional intermeddling with personal property, including the Electronic Devices, in the possession of another that results in the deprivation of the use of the personal property or impairment of the condition, quality, or usefulness of the personal property, or impairs some other legally protected interest, including the legally protected interest in privacy and confidential information.

100. By engaging in the acts alleged in this complaint without the authorization or consent of Plaintiff and Class Members, Defendant dispossessed Plaintiff and Class Members from use and/or access to their personal confidential information. Further, these acts impaired the use, value, and quality of Plaintiff and Class Members' personal confidential information. Defendant's acts constituted an intentional interference with the use and enjoyment of Plaintiff and Class Members' personal confidential information. By the acts described above, Defendant repeatedly and persistently engaged in trespass to personal property in violation of the common law.

101. Without Plaintiff and Class Members' authorization or consent, or in excess of any authorization or consent given, Defendant knowingly and intentionally accessed Plaintiff and Class Members' property, thereby intermeddling with Plaintiff and Class Members' right to exclusive possession of the property and causing injury to Plaintiff and the members of the Class.

102. Defendant engaged in deception and concealment to gain access to Plaintiff and Class Members' computers.

103. Defendant engaged in the following conduct with respect to Plaintiff and Class Members' Electronic Devices: Defendant accessed and obtained control over Plaintiff and Class Members' personal confidential information; Defendant caused the installation of Defendant's Carrier IQ software application on Plaintiff and Class

Members' Electronic Devices; Defendant deliberately programmed the operation of its software application code to bypass and circumvent the Electronic Device owners' privacy and security controls, to remain beyond their control, and to continue to function and operate without notice to them or consent from them. All these acts described above were acts in excess of any authority Plaintiff and Class Members granted when visiting websites and none of these acts was in furtherance of Plaintiff and Class Members' viewing the content or utilizing services on websites. By engaging in deception and misrepresentation, whatever authority or permission Plaintiff and Class Members may have granted to the Defendant did not apply to Defendant's conduct.

104. Defendant's installation and operation of its program used, interfered, and/or intermeddled with Plaintiff and Class Members' Electronic Devices. Such use, interference and/or intermeddling was without Plaintiff and Class Members' consent or, in the alternative, in excess of Plaintiff and Class Members' consent.

105. Defendant's installation and operation of its program constitutes trespass, nuisance, and an interference with Plaintiff and Class Members' chattels, to wit, their Electronic Devices and personal confidential information.

106. Defendant's installation and operation of its Carrier IQ software application impaired the condition and value of Plaintiff and Class Member's Electronic Devices and personal confidential information.

107. Defendant's trespass to chattels, nuisance, and interference caused real and substantial damage to Plaintiff and Class Members.

108. As a direct and proximate result of Defendant's trespass to chattels, nuisance, interference, unauthorized access of and intermeddling with Plaintiff and Class Members' property, Defendant has injured and impaired in the condition and value of Class Members' Electronic Devices and personal confidential information, as follows:

a. by consuming the resources of and/or degrading the performance of Plaintiff and Class Members' Electronic Devices (including hard drive space, memory, processing cycles, and Internet connectivity);

b. by diminishing the use of, value, speed, capacity, and/or capabilities of Plaintiff and Class Members' Electronic Devices;

c. by devaluing, interfering with, and/or diminishing Plaintiff and Class Members' possessory interest in their Electronic Devices and personal confidential information;

d. by altering and controlling the functioning of Plaintiff and Class Members' Electronic Devices and personal confidential information;

e. by infringing on Plaintiff and Class Members' right to exclude others from their Electronic Devices and personal confidential information;

f. by infringing on Plaintiff and Class Members' right to determine, as owners of their Electronic Devices, which programs should be installed and operating on their Electronic Devices;

g. by compromising the integrity, security, and ownership of Class Members' Electronic Devices and personal confidential information; and

h. by forcing Plaintiff and Class Members to expend money, time, and resources in order to remove the program installed on their Electronic Devices without notice or consent.

109. Defendant's conduct constituted an ongoing and effectively permanent impairment of Plaintiff and Class Members' Electronic Devices and personal confidential information.

110. Plaintiff and Class Members each had and have legally protected, privacy and economic interests in their Electronic Devices and personal confidential information.

///

///

111. Plaintiff and Class Members sustained harm as a result of Defendant's actions, in that the expected operation and use of their Electronic Devices and personal confidential information were altered and diminished on an ongoing basis.

112. As a direct and proximate result of Defendant's trespass to chattels, interference, unauthorized access of and intermeddling with Plaintiff and Class Members' Electronic Devices and personal confidential information, Plaintiff and Class Members have been injured, as described above.

113. Plaintiff, individually and on behalf of the Class, seek injunctive relief restraining Defendant from such further trespass to chattels and requiring Defendant to account for its use of Plaintiff and Class Members' Electronic Devices and personal confidential information, account for the personal information they have acquired, purge such data, and pay damages in an amount to be determined.

COUNT IV

Violation of the Unfair Competition Law ("UCL")
California Business and Professions Code § 17200, et seq.

114. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

115. By engaging in the above-described acts and practices, Defendant has committed one or more acts of unfair competition within the meaning of the UCL and, as a result, Plaintiff and the Class have suffered injury-in-fact and have lost money and/or property—specifically, personal confidential information and the full value of their Electronic Devices and personal confidential information.

116. Defendant's actions described above are in violation of California Business and Professions Code section 17500, et seq. and violations of the right of privacy enshrined in Article I, Section 1 of the Constitution of the State of California.

117. In addition, Defendant's business acts and practices are unlawful, because they violate the Electronic Communications Privacy Act and California Invasion of Privacy Act. Defendant is therefore in violation of the "unlawful" prong of the UCL.

118. Defendant's business acts and practices are unfair because they cause harm and injury-in-fact to Plaintiff and Class Members and for which Defendant has no justification. Defendant's conduct lacks reasonable and legitimate justification in that Defendant has benefited from such conduct and practices while Plaintiff and the Class Members have suffered material disadvantage regarding their interests in the privacy and confidentiality of their personal information. Defendant's conduct offends public policy in California tethered to the right of privacy set forth in the Constitution of the State of California, and California statutes recognizing the need for consumers to obtain material information with which they can take steps to safeguard their privacy interests.

119. Defendant's acts and practices were also fraudulent within the meaning of the UCL because they are likely to mislead the members of the public to whom they were directed.

120. As a result, Plaintiff and the Class have suffered and will continue to suffer damages.

121. Further, as a direct and proximate result of Defendant's willful and intentional actions, Plaintiff and the Class have suffered damages in an amount to be determined at trial and, unless Defendant is restrained, Plaintiff will continue to suffer damages.

COUNT V
STATUTORY INVASION OF PRIVACY IN VIOLATION OF CALIFORNIA PENAL CODE SECTIONS 631 AND 632.7

122. Plaintiff repeats and re-alleges each of the foregoing paragraphs as though fully set forth herein.

123. At all material times, Penal Code Sections 631 and 632.7 were in full force and effect and were binding upon Defendant, and existed for the benefit of the Class members, including Plaintiff, all of whom are and/or were protected by the California Invasion of Privacy Act (Penal Code §§ 630 *et seq*).

124. Plaintiff is informed, believes, and thereupon allege that Defendant willfully and without the consent of all parties to communications, or in some other unauthorized manner, read, or attempted to read, or to learn the contents or meaning of messages, reports, or communications while the same were in transit or passing over wires, lines, or cables, or were being sent from, or received at any place within California; or used, or attempted to use, in some manner, or for any purpose, or to communicate in any way, any information so obtained, or aided, agreed with, employed, or conspired with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned herein during the Class Period. (Cal. Pen. Code § 631(a).)

125. Plaintiff is further informed, believes, and thereupon alleges that Defendant, without the consent of all parties to the communication, intercepted or received and intentionally recorded, or assisted in the interception or reception and intentional recordation of, a communication transmitted by and between the Electronic Devices. (Cal. Pen. Code § 632.7(a).)

126. Penal Code Section 637.2 is a manifestation of the California Legislature's determination that the privacy invasion arising from the non-consensual interception, wiretapping, eavesdropping, or recording of a confidential communication constitutes an affront to human dignity that warrants a minimum of $5,000 in statutory damages per violation, even in the absence of proof of actual damages, as well as injunctive relief enjoining further violations. (Cal. Pen. Code § 637.2(a)-(c).) Defendant's unlawful conduct caused injury to Plaintiff and the Class in the form of an affront to their human dignity.

127. Based upon the foregoing, the Class members, including the Plaintiff, are entitled to, and below do pray for, statutory damages for each of Defendant's violations of Penal Code Sections 631, 632.7 and for injunctive relief, as provided under Penal Code Section 637.2.

///

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays that this Court:

a. Certify this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, appoint the named Plaintiff as the Class representative, and appoint the undersigned as class counsel;

b. Order Defendant to pay Plaintiff and other members of the Class an amount of actual and statutory damages, restitution and punitive damages in an amount to be determined at trial;

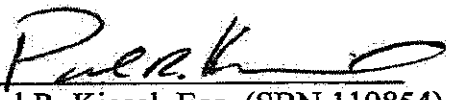
c. Issue a permanent injunction or other appropriate equitable relief requiring Defendant refrain from its ongoing illegal interception and other activities;

d. Issue an order granting Plaintiff's reasonable costs and attorney's fees; and

e. Grant such other relief as may be just and proper.

Dated: December 13, 2011

KIESEL BOUCHER LARSON LLP

By: 

Paul R. Kiesel, Esq. (SBN 119854)
KIESEL BOUCHER LARSON LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Telephone: (310) 854-4444
Facsimile: (310) 854-0812

Paul O. Paradis, Esq.
Gina M. Tufaro, Esq
Mark A. Butler, Esq.
pparadis@hhplawny.com
HORWITZ, HORWITZ & PARADIS, Attorneys at Law
570 Seventh Avenue, 20th Floor
New York, NY 10018
Telephone: (212) 986-4500
Facsimile: (212) 986-4501

James v. Bashian, Esq.
Law Offices of James V. Bashian
500 Fifth Avenue – Suite 2700
New York, New York
Telephone: (212) 921-4110

Jay P. Saltzman, Esq.
Law Offices of Jay Saltzman, P.C.
110 Wall Street, 11th Floor
New York, NY 10005
Telephone: (646) 374-4282

Counsel for Plaintiff

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury on all issues so triable.

Dated: December 13, 2011

KIESEL BOUCHER LARSON LLP

By: _____

Paul R. Kiesel, Esq. (SBN 119854)
KIESEL BOUCHER LARSON LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Telephone: (310) 854-4444
Facsimile: (310) 854-0812

Paul O. Paradis, Esq.
Gina M. Tufaro, Esq
Mark A. Butler, Esq.
pparadis@hhplawny.com
HORWITZ, HORWITZ & PARADIS, Attorneys at Law
570 Seventh Avenue, 20th Floor
New York, NY 10018
Telephone: (212) 986-4500
Facsimile: (212) 986-4501

James v. Bashian, Esq.
Law Offices of James V. Bashian
500 Fifth Avenue – Suite 2700
New York, New York
Telephone: (212) 921-4110

Jay P. Saltzman, Esq.
Law Offices of Jay Saltzman, P.C.
110 Wall Street, 11th Floor
New York, NY 10005
Telephone: (646) 374-4282

Counsel for Plaintiff